



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/720,447	11/25/2003	Tom Cheng	13914-033001 / 2003P00877	4999
32864	7590	06/15/2009		
FISH & RICHARDSON, P.C. PO BOX 1022 MINNEAPOLIS, MN 55440-1022				
EXAMINER				
ZEE, EDWARD				
ART UNIT		PAPER NUMBER		
2435				
NOTIFICATION DATE		DELIVERY MODE		
06/15/2009		ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Office Action Summary

Application No.

10/720,447

Applicant(s)

CHENG ET AL.

Examiner

EDWARD ZEE

Art Unit

2435

Period for Reply -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 February 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4, 7-11, 13-16, 19 and 20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4, 7-11, 13-16, 19 and 20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/808)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This is in response to the amendments filed on February 20th, 2009. Claims 1-4, 8-11, 13-16 and 19 have been amended; Claims 1-4, 7-11, 13-16, 19 and 20 are pending and have been considered below.
2. The indicated potential allowability of the claims is withdrawn due to the apparent change in scope of the newly amended independent claims. The Examiner respectfully submits that the pending claims not only appear to encompass a slightly different scope, but also appear to be broader in scope than the previously present set of claims. Therefore, upon further reconsideration, the previous grounds of rejections (ie. Wong et al.) have been reapplied below. Additionally, in the interest of expediting prosecution, an additional art rejection based upon an alternate rationale has been presented below as well.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
4. **Claims 1-4, 7-11, 13-16, 19 and 20** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
5. **Claim 1** recites the limitation "*the attribute*" in line 26. There is insufficient antecedent basis for this limitation in the claim. The Examiner notes that there are a slew of "attributes" recited in the instant claim, such as but not limited to: "multiple attributes", "permission attributes", "attributes" in the attribute access group, an "attribute" of the multiple attributes

associated with the data object which is consistent with the permission value, etc. Therefore, it is unclear exactly which "attribute" the instant limitation is in reference to.

6. **Claim 1** recites the limitation *"the data object that the user seeks to access"* in line 27. There is insufficient antecedent basis for this limitation in the claim. The Examiner notes that this appears to be in reference to the "data object" recited in line 7; however upon further consideration of the entire claim as a whole, this may or may not be the case, as the Applicant explicitly makes reference to "the data object" throughout the instant claim. Therefore, it is unclear if a separate instance of a data object is actually being claimed.

7. **Claim 1** recites the limitation *"the attribute sought to be accessed"* in lines 31-32. There is insufficient antecedent basis for this limitation in the claim. The Examiner notes that the instant claim appears to be drawn towards seeking access to a data object (or a part of the data object), and thus is unclear if the Applicant is also attempting to claim the aspect of seeking access to a particular attribute as well.

8. The Examiner notes that the issues noted above with respect to Claim 1 appear to exist in the remaining independent claims as well. Therefore, the Applicant is kindly requested to clarify such issues in regards to the remaining claims which were not directly addressed above.

Claim Rejections - 35 USC § 101

9. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 8-11 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 8-11 recite a method for determining whether a user is

permitted to access a business object. While the claims recite a series of steps or acts to be performed, a statutory “process” under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of *In Re Bilski* 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The instant method including steps of “*using a permission object to determine whether a user associated with an entry in user information is permitted access...*”, “*allowing/denying access...*” and the like are broad enough that the claims could be completely performed mentally, verbally or without a machine nor is any transformation apparent. For example, the “determining” step can be performed mentally by a human, and the “allowing/denying access” step can be performed verbally.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. **Claims 1-4, 7-11, 13-16 and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Wong et al. (6,578,037).**

Claims 1 and 8: Wong et al. discloses a method and computer-readable medium having embodied thereon a computer program configured to determine whether a user is permitted to access a business object when executing a software application of an enterprise information technology system, the medium storing one or more code segments configured to:

a. use a permission object(*ie. policy group attribute*) to determine whether a user associated with an entry in user information is permitted to access a data object associated with a data object type(*ie. objects 218 and 224*) [figure 2];

b. wherein the entry in the user information(*ie. context information*) associates the user with a user affiliation [column 6, lines 51-67], the permission object identifies:

i. a user affiliation(*ie. which policy group user is associated to*) to which the permission object applies [column 6, lines 3-9];

ii. a data object type(*ie. type of database record*) to which the permission object applies such that the data object type is associated with multiple attributes(*ie. salary range, job categories, etc.*) and each data object having the data object type identified by the permission object is associated with the multiple attributes [column 6, lines 29-39];

iii. a permission attribute(*ie. salary range, job categories, etc.*) identifying at least one of the multiple attributes [column 6, lines 29-39];

iv. a permission value(*ie. employee's salary, employee's job category, etc.*) for the permission attribute [column 6, lines 29-39];

v. and an attribute access group having one or more attributes of the multiple attributes associated with the data object type identified by the permission object [column 5, lines 40-51];

c. wherein the user is permitted to access the attribute sought to be accessed upon determination that:

i. the user affiliation that is associated with the user is the same user affiliation as the user affiliation to which the permission object applies(*ie. users affiliated with the "Human Resources of Company A" policy group may access employee records of employees earning salaries below a threshold*) [column 6, lines 29-39];

ii. the data object type(*ie. only Company A's records*) of the data object is the same as the data object type to which the permission object applies [column 6, lines 29-39];

iii. a value(*ie. recorded salary of employee's record is within the range of accessible salaries*) of an attribute of the multiple attributes associated with the data object is consistent with the permission value of the permission attribute and the attribute corresponds to the permission attribute [column 6, lines 29-39];

iv. and at least one attribute of the data object that the user seeks to access corresponds to an attribute of the attribute access group of the permission object(*ie. returning query results which are allowed by the particular policy, etc.*) [column 5, lines 40-51];

d. and wherein otherwise the user is denied access to the attribute sought to be accessed(*ie. restrict results returned by a query, thereby restricting access to data*) [column 5, lines 40-51].

Claim 13: Wong et al. discloses a computer system for determining whether a user is permitted to access a data object when executing a software application of an enterprise information technology system, the system tangibly embodied and comprising:

- a. a processor;
- b. a storage device including a data repository(*ie. database system 100*) for access control information for software having data objects, each data object [figure 1]:
 - i. being associated with a data object type(*ie. only Company A's records*) having multiple attributes(*ie. salary ranges, job categories, etc.*) [column 6, lines 29-39];
 - ii. having the multiple attributes(*ie. salary range, job categories, etc.*) of the data object type to which the data object is associated [column 6, lines 29-39];
 - iii. and having a value associated(*ie. employee's salary, employee's job category, etc.*) with each attribute of the multiple attributes [column 6, lines 29-39];
- c. the data repository including:
 - i. user information(*ie. context attribute values*) that associates a user affiliation with a user of the software application [column 7, lines 46-48];
 - ii. and permission information(*ie. Company A HR policy group*) having multiple permission objects(*ie. policies*), each permission object identifying a user affiliation(*ie. only users from Company A's HR department*) to which the permission object applies, a data object type(*ie. only Company A's employee records*) to which the permission object applies, a permission attribute(*ie. salary range*) identifying one of the multiple attributes, a permission value(*ie. employee's salary*) for the permission attribute [column 6, lines

29-39], and an attribute access group having one or more attributes of the multiple attributes of the data object type [column 5, lines 40-51];

d. and an executable software module executed by the processor that causes:

i. a comparison of a value of an attribute of the multiple attributes of a data object to which a user seeks access such that the attribute of the multiple attributes corresponds to the permission attribute of a permission object with the permission value of the permission object(*ie. conditions that restrict results returned by a query, thereby restricting access to data*) [column 5, lines 49-50];

ii. a comparison of at least one attribute of the data object that the user seeks to access such that the attribute sought to be accessed corresponds to an attribute of the attribute access group of the permission object [column 5, lines 40-51];

iii. and an indication that a user is permitted to access the attribute sought to be accessed when:

1. the value of the attribute of the data object is consistent with the permission value of the permission object(*ie. the function checks context value attributes that identify the user to determine whether the users is associated with company A*) [column 7, lines 41-45];

2. and at least one attribute of the data object that the user seeks to access corresponds to an attribute of the attribute access group of the permission object(*ie. returning query results which are allowed by the particular policy, etc.*) [column 5, lines 40-51];

e. and wherein otherwise the user is denied access to the attribute sought to be accessed(*ie. restrict results returned by a query, thereby restricting access to data*) [column 5, lines 40-51].

Claims 2, 9 and 14: Wong et al. discloses a medium, method and system of claims 1, 8 and 13 and further discloses that the one or more code segments are further configured to permit the user to access the data object when the value of the attribute of one of the multiple attributes associated with the data object is the same as the permission value of the permission attribute(*ie. permit users in HR of Company A to access employee records of employees earning salaries below a threshold*) [column 6, lines 29-39].

Claims 3, 10 and 15: Wong et al. discloses a medium, method and system of claims 1, 8 and 13 and further discloses that the one or more code segments are further configured to permit the user to access the data object when the value of the attribute of one of the multiple attributes associated with the data object is the within a range specified(*ie. range of salaries below a threshold*) by the permission value of the permission attribute [column 6, lines 29-39].

Claims 4, 11 and 16: Wong et al. discloses a medium, method and system of claims 1, 8 and 13 and further discloses that the one or more code segments are further configured to permit the user to access the data object when the value of the attribute of one of the multiple attributes associated with the data object is one of enumerated values(*ie. one of the particular job categories*) specified by the permission value of the permission attribute [column 6, lines 29-39].

Claims 7 and 19: Wong et al. discloses a medium or signal and system of claims 1 and 13 and further discloses that the permission object identifies a permitted action(*ie. access rule of particular context attribute value allows users associated with company A to change policy*

group attributes), and the one or more code segments are further configured to permit the user to access the data object and perform an action on the data object when the action is consistent with the permitted action identified in the permission object(*ie. the function checks context value attributes that identify the user to determine whether the user is associate with company A, and whether the new value belongs to the particular set of values*) [column 7, lines 30-45].

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

13. **Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al. (6,578,037) in view of Kraenzel (6,513,039).**

Claim 20: Wong et al. discloses a medium of claim 1 and further discloses that the permission object identifies a permitted action(*ie. access rule of particular context attribute value allows users associated with company A to change policy group attributes*), and the one or more code segments are further configured to permit the user to access the data object and perform an action on the data object when the action is consistent with the permitted action identified in the permission object(*ie. the function checks context value attributes that identify the user to determine whether the user is associate with company A, and whether the new value belongs to the particular set of values*) [column 7, lines 30-45], but does not explicitly disclose that the

actions are database operations wherein the database operations comprise of: create, read, update and delete.

However, Kraenzel discloses a similar invention and further discloses various database access operations such as read-only, edit or the like [column 1, lines 12-26].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the invention disclosed by Wong et al. with the additional features of Kraenzel, in order to prevent access to sensitive objects such as those containing confidential information, as suggested by Kraenzel.

Claim Rejections - 35 USC § 102 (Based upon alternate rationale)

14. Claims 1-4, 7-11, 13-16, 19 and 20 are rejected under 35 U.S.C. 102(b) as being anticipated by Keisuke et al. (EP 0 992 873 A2).

Claims 1 and 8: Keisuke et al. discloses a method and computer-readable medium having embodied thereon a computer program configured to determine whether a user is permitted to access a business object when executing a software application of an enterprise information technology system, the medium storing one or more code segments configured to:

- a. use a permission object(*ie. ACL file*) to determine whether a user associated with an entry in user information is permitted(*ie. allow*) to access a data object associated with a data object type [figure 6];
- b. wherein the entry in the user information associates the user with a user affiliation(*ie. general manager, section chief, system manager, ordinary members, etc.*) [figure 4], the permission object identifies:

- i. a user affiliation to which the permission object applies(*ie. abstract user names*) [column 5, paragraph 0034];
 - ii. a data object type(*ie. registers sports related information as content 28 etc.*) to which the permission object applies such that the data object type is associated with multiple attributes and each data object having the data object type identified by the permission object is associated with the multiple attributes [column 18, paragraph 0143];
 - iii. a permission attribute identifying at least one of the multiple attributes(*ie. departments 3, 4, etc.*) [column 18, paragraph 0143];
 - iv. a permission value for the permission attribute(*ie. sports, movie, etc.*) [column 18, paragraph 0143];
 - v. and an attribute access group having one or more attributes of the multiple attributes associated with the data object type identified by the permission object(*ie. access-rights, etc.*) [figure 16];
- c. wherein the user is permitted to access the attribute sought to be access upon determination that:
- i. the user affiliation that is associated with the user is the same user affiliation as the user affiliation to which the permission object applies [column 18, paragraphs 0142-0147];
 - ii. the data object type of the data object is the same as the data object type to which the permission object applies [column 18, paragraphs 0142-0147];

iii. a value of an attribute of the multiple attributes associated with the data object is consistent with the permission value of the permission attribute and the attribute corresponds to the permission attribute [column 18, paragraphs 0142-0147];

iv. and at least one attribute of the data object that the user seeks to access corresponds to an attribute of the attribute access group of the permission object [column 18, paragraphs 0142-0147];

d. and wherein otherwise the user is denied access to the attribute sought to be accessed (*ie. users with a rank A can vote, users with a rank B cannot vote, etc.*) [figure 16].

Claim 13: Keisuke et al., discloses a computer system for determining whether a user is permitted to access a data object when executing a software application of an enterprise information technology system, the system tangibly embodied and comprising:

a. a processor;

b. a storage device including a data repository for access control information for software having data objects, each data object:

i. being associated with a data object type (*ie. registers sports related information as content 28, etc.*);

ii. having the multiple attributes of the data object type to which the data object is associated [figure 3];

iii. and having a value associated with each attribute of the multiple attributes [figure 3];

c. the data repository including:

- i. user information that associates a user affiliation with a user of the software application(*ie. abstract user name, etc.*) [column 9, paragraph 0068];
- ii. and permission information having multiple permission objects(*ie. ACL file*), each permission object identifying a user affiliation to which the permission object applies, a data object type to which the permission object applies, a permission attribute identifying one of the multiple attributes(*ie. departments 3, 4, etc.*), a permission value for the permission attribute(*ie. sports, movie, etc.*), and an attribute access group(*ie. access-rights, etc.*) having one or more attributes of the multiple attributes of the data object type [figure 6];
- d. and an executable software module executed by the processor that causes:
 - i. a comparison of a value of an attribute of the multiple attributes of a data object to which a user seeks access such that the attribute of the multiple attributes corresponds to the permission attribute of a permission object with the permission value of the permission object [column 18, paragraphs 0142-0147];
 - ii. a comparison of at least one attribute of the data object that the user seeks to access such that the attribute sought to be accessed corresponds to an attribute of the attribute access group of the permission object [column 18, paragraphs 0142-0147];
 - iii. and an indication that a user is permitted to access the attribute sought to be accessed when:
 - 1. the value of the attribute of the data object is consistent with the permission value of the permission object [column 18, paragraphs 0142-0147];

2. and at least one attribute of the data object that the user seeks to access corresponds to an attribute of the attribute access group of the permission object [column 18, paragraphs 0142-0147];

e. and wherein otherwise the user is denied access to the attribute sought to be accessed(*ie. users with a rank A can vote, users with a rank B cannot vote, etc.*) [figure 16].

Claims 2, 9 and 14: Keisuke et al. discloses a medium, method and system of claims 1, 8 and 13 and further discloses that the one or more code segments are further configured to permit the user to access the data object when the value of the attribute of one of the multiple attributes associated with the data object is the same as the permission value of the permission attribute(*ie. sports-related information, etc.*) [column 18, paragraphs 0142-0147].

Claims 3, 10 and 15: Keisuke et al. discloses a medium, method and system of claims 1, 8 and 13 and further discloses that the one or more code segments are further configured to permit the user to access the data object when the value of the attribute of one of the multiple attributes associated with the data object is the within a range specified(*ie. in the range of their rights...*) [column 19, paragraph 0154].

Claims 4, 11 and 16: Keisuke et al. discloses a medium, method and system of claims 1, 8 and 13 and further discloses that the one or more code segments are further configured to permit the user to access the data object when the value of the attribute of one of the multiple attributes associated with the data object is one of enumerated values specified by the permission value of the permission attribute(*ie. ranks, etc.*) [column 18, paragraphs 0142-0147].

Claims 7 and 19: Keisuke et al. discloses a medium or signal and system of claims 1 and 13 and further discloses that the permission object identifies a permitted action, and the one or more

code segments are further configured to permit the user to access the data object and perform an action on the data object when the action is consistent with the permitted action identified in the permission object(*ie. read, vote, etc.*) [column 18, paragraphs 0142-0147].

Claim 20: Keisuke et al., discloses a medium of claim 1 and further discloses that the permission object identifies a permitted action, and the one or more code segments are further configured to permit the user to access the data object and perform one or more database operations on the data object when the action is consistent with the permitted action identified in the permission object, where the database operations comprise of: create, read, update and delete [figure 3].

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. David et al. (6,457,130).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EDWARD ZEE whose telephone number is (571)270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
June 4, 2009
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435